



Recommended Practices on Notification of Security Breach Involving Personal Information

October 10, 2003

Joanne McNabb, Chief
Office of Privacy Protection
California Department of Consumer Affairs
www.privacy.ca.gov

Contents

Introduction	5
California Law	7
Recommended Practices	8
Part 1: Protection and Prevention	8
Part II: Preparation for Notification	10
Part III: Notification	11
End Notes	14
Appendix 1: Advisory Group List	17
Appendix 2: Sample Notice Letters	19
Appendix 3: California Law	23
Appendix 4: Reporting to Law Enforcement	27
Appendix 5: Information Security Resources	31
Appendix 6: Benchmark Study	33

Recommended Practices on Notification of Security Breach

Introduction

The Office of Privacy Protection in the California Department of Consumer Affairs has the statutorily mandated purpose of “protecting the privacy of individuals’ personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices.”¹ Among other things, the law specifically directs the Office to “make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers.”²

In fulfillment of those obligations, the Office of Privacy Protection is publishing these recommended practices for providing notice in cases of security breach involving personal information.

In developing the recommendations, the Office of Privacy Protection received consultation and advice from an advisory group made up of representatives of the financial, health care, retail, technology and information industries; state government agencies; law enforcement; and consumer privacy advocates.³ The group members’ contributions were very helpful and are greatly appreciated.

Identity Theft

We now know that identity theft is much more common than reports in recent years suggested. A national survey conducted by the Federal Trade Commission found that the number of victims in 2002 approached 10 million, and two other recent surveys estimated the number at seven million.⁴ That’s nearly 10 times greater than the previously quoted estimate of less than a million a year. If the same rate is applied to California, then over a million Californians became victims of identity theft in the past year.

The surveys also confirmed the opinions of law enforcement and others that identity theft is on the

rise in the U.S., showing a dramatic increase between 2001 and 2002.⁵

The costs of the crime are alarming. Recent studies estimate the average victim’s out-of-pocket expenses at \$500 to \$740, and the time spent clearing up the situation at from 30 to several hundred hours.⁶ The Federal Trade Commission estimates the total annual cost to business as \$50 billion for 2002, based on an average loss from the misuse of a victim’s personal information of \$4,800.⁷

Studies also show that the cost of an identity theft incident, both for victims and for business, is significantly lower if it is discovered quickly.⁸

Security Breaches

Security is an essential component of information privacy. It is one of the basic principles of fair information practice: Organizations that collect or manage individuals’ personal information should use security safeguards to protect that information against unauthorized access, use, disclosure, modification or destruction.⁹ Implementing an effective information security program is essential for an organization to fulfill its responsibility towards the individuals who entrust it with their personal information. It is the best way to reduce the risk of exposing individuals to the possibility of identity theft. It is also the best way to reduce the risk of exposing the organization to the cost of an information security breach to its reputation and finances.

Most business and all government agencies today acknowledge their responsibility for ensuring the security of the personal information in their care. In its 2000 report to Congress on the privacy practices of companies doing business online, the Federal Trade Commission found that the privacy policies of 74 percent of the 100 most popular Web sites included a statement that they took steps to provide security for the information they collected.¹⁰ Many

organizations in the U.S. are legally required to protect the security of personal information. The two major federal laws on privacy enacted in recent years—the Gramm-Leach-Bliley Act and the Health Information Portability and Accountability Act—include security rules that apply to a broad range of financial institutions and health care organizations.¹¹ The California Information Practices Act requires government agencies to establish safeguards to ensure the security and confidentiality of records.¹²

Nevertheless, information security studies have indicated that the number of breaches has increased over time, along with their frequency, severity and the costs to business of responding.¹³ One recent survey found that 39 percent of the large global financial institutions responding acknowledged that their systems had been compromised in the past year, although the researcher commented that the figure seemed low compared to other surveys showing that nearly 80 to 90 percent of Fortune 500 companies and government agencies have experienced breaches.¹⁴

California, which leads the nation in privacy protection statutes, has recently enacted a law to address this situation. The law is intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to mitigate the crime's impact.

In order to get an early look at how a number of major corporations had prepared to implement the new California law on notification of security breach, the Ponemon Institute conducted a preliminary benchmark survey in early July 2003, as the law first took effect.¹⁵ The study suggests that corporations have been prompted to take action by the law, including acquiring enabling technologies to protect their information technology infrastructure from data breaches, and that the law does not create a significant cost-of-compliance burden. The study also revealed some areas where best practice guidance was sought, such as encryption and coordination of notification responsibilities of third parties with whom data is shared.

California Law on Notification of Security Breach

California Civil Code Sections 1798.29 and 1798.82 to 1798.84 apply to any person or business in California and to government agencies. The full text of the law is attached as Appendix 3. The main provisions are summarized below.

Security Breach

- Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.

Type of Information

- Unencrypted computerized data including certain personal information.
- Personal information that triggers the notice requirement is name (first name or initial and last name) plus any of the following:
 - Social Security number,
 - Driver's License or California Identification Card number, OR
 - Financial account number, credit or debit card number (along with any PIN or other access code where required for access to account).

How to Notify

- Notice may be provided in writing, electronically (as consistent with provisions on electronic records and signatures per 15 USC 7001), or by substitute notice.
- Substitute notice may be used if the cost of providing individual notice is >\$250,000 or if >500,000 people would have to be notified. Substitute notice means all of the following:
 - E-mail when the e-mail address is available, and
 - Conspicuous posting on agency web site, and
 - Notification of major statewide media.
- Alternatively, the business or agency may use its own notification procedures as part of an information security policy for personal information, if its procedures are consistent with the timing requirements of the law and if it notifies subjects in accordance with its policy.

Whom to Notify

- Notice must be given to any data subjects who are California residents.

When to Notify

- Timing: "in the most expedient time possible and without unreasonable delay." Time may be allowed for the following:
 - Legitimate needs of law enforcement if notification would impede a criminal investigation
 - Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system.

Recommended Practices

The Office of Privacy Protection's recommendations are intended to assist organizations in supplementing their information security programs. The recommendations are not regulations and are not binding. Nor are they limited to the scope of the California law on notice of security breach, but rather they represent a broader approach and a higher standard.

These "best practices" recommendations can serve as guidelines for organizations, to assist them in providing timely and helpful information to individuals whose personal information has been compromised while in the organization's care. Unlike many best practices sets, however, these recommendations do not contain all the practices that should be observed. Information-handling practices and technology are changing rapidly, and organizations should continuously review and update their own situation to ensure compliance with the laws and principles of privacy protection. It is recognized that specific or unique considerations, including compliance with other laws, may make some of these practices inappropriate for some organizations.

Our practice recommendations are presented in three parts: Part I - Protection and Prevention, Part II - Preparation for Notification, and Part III - Notification. While the California law on notice of security breach applies only to records in electronic media ("computerized data") and defines a limited set of items of personal information as triggering the notification requirement, we recommend applying these practices to records in any media, including paper records.

Definitions

The following are the definitions of key terms used in these recommended practices.

Notice-triggering information: As provided in California law, this is unencrypted, computerized first name or initial and last name plus any of the following: Social Security number, driver's license number, California Identification Card number, or

financial account number, credit or debit card number, in combination with any code or password permitting access to an individual's financial account where such a code or password is required.

Higher-risk personal information: Not only the notice-triggering information that could subject an individual to identity theft, but also health information, other financial information and other personal information the disclosure of which would violate the privacy of individuals.

Data owner: The individual or organization with primary responsibility for determining the purpose and function of a record system.

Data custodian: The individual or organization that has responsibility delegated by the data owner for maintenance and technological management of the record system.

Part 1: Protection and Prevention

While an organization's information security program may be unique to its situation, there are recognized basic components of a comprehensive, multi-layered program to protect personal information from unauthorized access.¹⁶ An organization should protect the confidentiality of personal information whether it pertains to customers, employees or others. For both paper and electronic records, these components include physical, technical and administrative safeguards. Among such safeguards are the following recommended practices.

1. Collect the minimum amount of personal information necessary to accomplish your business purposes, and retain it for the minimum time necessary.
2. Inventory records systems, critical computing systems and storage media to identify those containing personal information.
 - Include laptops and handheld devices used to store personal information.

3. Classify personal information in records systems according to sensitivity.
 - Identify notice-triggering information.
4. Use physical and technological security safeguards as appropriate to protect personal information, particularly higher-risk information such as Social Security number, driver's license number, California Identification Card number, financial account numbers and any associated passwords and PIN numbers, other financial information, and health information, in paper as well as electronic records.
 - Authorize employees to have access to only the specific categories of personal information their job responsibilities require.
 - Where possible, use technological means to restrict internal access to specific categories of personal information.
 - Monitor employee access to higher-risk personal information.
 - Remove access privileges of former employees and contractors immediately.
5. Promote awareness of security and privacy policies and procedures through ongoing employee training and communications.
 - Monitor employee compliance with security and privacy policies and procedures.
 - Include all new, temporary, and contract employees in security and privacy training and monitoring.
 - Impose penalties for violation of security and privacy policies and procedures.
6. Require third-party service providers and business partners who handle personal information on behalf of your organization to follow your security policies and procedures.
 - Make privacy and security obligations of third parties enforceable by contract.
7. Use intrusion detection technology and procedures to ensure rapid detection of unauthorized access to higher-risk personal information.
 - Conduct periodic penetration tests to determine effectiveness of systems and staff procedures in detecting and responding to security breaches.
8. Wherever feasible, use data encryption, in combination with host protection and access control, to protect higher-risk personal information.
 - Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard.¹⁷
9. Dispose of records and equipment containing personal information in a secure manner, such as shredding paper records with a cross-cut shredder and using a program to "wipe" and overwrite the data on hard drives.¹⁸
10. Review your security plan at least annually or whenever there is a material change in business practices that may reasonably implicate the security of personal information. For example, if an organization decides to outsource functions that use personal information, such as using a call center, the plans should be revisited to take the new third parties into account.

Part II: Preparation for Notification

An information security program should include an incident response plan, which addresses security incidents including unauthorized access to or acquisition of higher-risk personal information.¹⁹ To ensure timely notice to affected individuals when appropriate, the following practices are among those that should be included in an incident response plan:

1. Adopt written procedures for internal notification of security incidents that may involve unauthorized access to higher-risk personal information.
2. Designate one individual as responsible for coordinating your internal notification procedures.
3. Regularly train employees, including all new, temporary and contract employees, in their roles and responsibilities in your incident response plan.
 - Collect 24/7 contact numbers for incident response team and provide to team members.
4. Define key terms in your incident response plan and identify responsible individuals.
5. Plan for and use measures to contain, control and correct any security incident that may involve higher-risk personal information.
6. Require the data custodian or others who detect an information security incident to immediately notify the data owner upon the detection of any security incident that may involve unauthorized access to the record system.
7. Require third-party service providers and business partners to adopt and follow your security incident notification procedures.
 - Monitor and contractually enforce third party compliance with your security incident response procedures.
8. Identify appropriate law enforcement contacts to notify on security incidents that may involve illegal activities. Appropriate law enforcement agencies include California's regional high-tech crimes task forces, the Federal Bureau of Investigation, the U.S. Secret Service, the National Infrastructure Protection Center, and the local police or sheriff's department. See Appendix 4, page 27, for contact information.
9. Consider suggestions from law enforcement with expertise in investigating high-technology crimes for inclusion in your incident response plan.²¹
10. Be sure to collect contact information (mailing address and/or e-mail address) from individuals whose notice-triggering personal information you collect or manage.
 - If you plan to contact affected individuals by e-mail, get the individuals' prior consent to the use of e-mail for that purpose, as provided in the federal Electronic Signature Act.²²
11. Adopt written procedures for notification of individuals whose unencrypted notice-triggering personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.
 - Include unauthorized acquisition of computer printouts and other paper records containing notice-triggering personal information in your notification procedures.
12. Document response actions taken on an incident. This will be useful to your organization and to law enforcement, if involved.
 - At the conclusion of an incident, review events and actions and make any indicated changes in your technology and response plan.
13. Review incident response plan at least annually or whenever there is a material change in your business practices that may reasonably implicate the security of personal information.

Part III: Notification

Openness or transparency is another basic privacy principle. An organization that collects or manages personal information should be open about its information policies and practices.²³ This responsibility includes informing individuals about incidents such as security breaches that have caused their unencrypted personal information to be acquired by unauthorized persons. The purpose of notifying individuals of such incidents is to enable them to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm.

To ensure giving timely and helpful notice to affected individuals, the following practices are recommended.

Acquisition: In determining whether unencrypted notice-triggering information has been *acquired*, or is reasonably believed to have been acquired, by an unauthorized person, consider the following factors, among others:

1. Indications that the information is *in the physical possession and control* of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information.
2. Indications that the information has been *downloaded* or copied.
3. Indications that the information was *used* by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Timing of Notification: Notify affected individuals in the most expedient time possible after the discovery of an incident involving unauthorized access to notice-triggering information.

1. Take necessary steps to contain and control the systems affected by the breach and conduct a preliminary internal assessment of the scope of the breach.
2. Once you have determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person, notify affected individuals within 10 business days. Do this unless law enforcement authorities tell you

that providing notice at that time would impede their investigation.

Contacting Law Enforcement: If you believe that the incident may involve illegal activities, report it to appropriate law enforcement agencies.²⁴

1. In contacting law enforcement, inform the law enforcement official in charge of the investigation that you intend to notify affected individuals within 10 business days as above.
2. If the law enforcement official in charge tells you that giving notice within that time period would impede the criminal investigation:
 - Ask the official to inform you as soon as you can notify the affected individuals without impeding the criminal investigation.
 - It should not be necessary for a law enforcement agency to complete an investigation before notification can be given.
 - Be prepared to send the notices immediately upon being so informed.

Whom to Notify: If your assessment leads you to reasonably believe that notice-triggering information was acquired by an unauthorized person, implement your notification plan.

1. Notify California residents whose notice-triggering information was acquired by an unauthorized person.
2. Notify affected individuals in situations involving unauthorized acquisition of notice-triggering information in any format, including computer printouts and other paper records.
3. Consider providing notice in breaches involving higher-risk personal information, even when it is not “notice-triggering” information under California law, if being notified would allow individuals to take action to protect themselves from possible harm.
4. If you cannot identify the specific individuals whose notice-triggering information was acquired, notify all those in the groups likely to

have been affected, such as all whose information is stored in the files involved.

5. Avoid false positives. A false positive occurs when the required notice of a security breach is sent to individuals who should not receive it because their personal information was not acquired as part of the breach. Consider the following when identifying the group that will be notified:
 - Before sending individual notices, make reasonable efforts to include only those individuals whose notice-triggering information was acquired.
 - Implement procedures for determining who gets included in the notice and who does not. Check the mailing list before sending the notice to be sure it is not over-inclusive.
 - Document your process for determining inclusion in the group to be notified.

Coordination with Credit Reporting Agencies:

Consumer credit reporting agencies (Equifax, Experian, and TransUnion) can help you give affected individuals information on the best ways for them to contact the agencies. A breach involving a large number of individuals can potentially have a significant impact on consumer reporting agencies and their ability to respond efficiently. High volumes of calls could impede access to the agencies. Be sure to contact the agencies before you send out notices in cases involving a large number of individuals—10,000 or more.

1. Make arrangements with the credit reporting agencies during your preparations for giving notice, without delaying the notice for this reason.
2. Organizations should contact the consumer credit reporting agencies as follows.
 - **Experian:** E-mail to BusinessRecordsVictimAssistance@experian.com.
 - **Equifax:** Chris Jarrard, Vice President - US Customer Services, Equifax Information Services, LLC, Phone: 678-795-7090, E-mail: chris.jarrard@equifax.com.

- **TransUnion:** E-mail to fvad@transunion.com, with “Database Compromise” as subject.

Contents of Notice: Sample notice letters are attached as Appendix 2. Include the following information in your notice to affected individuals:

1. A general description of what happened.
2. The nature of the individual’s personal information that was involved (not the Social Security number or other actual items of information).
3. What you have done to protect the individual’s personal information from further unauthorized acquisition.
4. What your organization will do to assist individuals, including providing an internal contact telephone number, preferably toll-free, for more information and assistance.
5. Information on what individuals can do to protect themselves from identity theft, including contact information for the three credit reporting agencies.
6. Contact information for the California Office of Privacy Protection and/or the Federal Trade Commission for additional information on protection against identity theft.
 - California Office of Privacy Protection
866-785-9663
www.privacy.ca.gov
 - Federal Trade Commission
877-ID-THEFT/877-438-4338
www.consumer.gov/idtheft/

Form and Style of Notice: Make the notice clear, conspicuous and helpful.

1. Use clear, simple language, guiding subheads, and plenty of white space in the layout.
2. Avoid jargon or technical language.
3. Avoid using a standardized format, which could result in making the public complacent about the process and thus undercut the purpose of the notice.

4. To avoid confusion, the notice should be a stand-alone document, not combined as part of another mailing.

Means of Notification: Individual notice to those affected is preferable whenever possible.

1. Send the notice to all affected individuals by first class mail.
2. Or notify by e-mail, if you normally communicate with the affected individuals by e-mail and you have received the prior consent of the individuals to that form of notification.
3. If more than 500,000 individuals were affected or if the cost of giving individual notice to affected individuals is greater than \$250,000 and you are using the “substitute notice” procedures:
 - Send the notice by e-mail to all affected parties whose e-mail address you have; AND
 - Post the notice conspicuously on your web site; AND
 - Notify major statewide media (television, radio, print).

End Notes

¹ California Business & Professions Code section 350(a).

² California Business & Professions Code section 350(c).

³ A list of the members of the advisory group is attached as Appendix 1.

⁴ The Federal Trade Commission (FTC)'s, *Identity Theft Survey Report* of September 2003, estimated that 4.6% of American adults were victims in 2002, is available at <<http://www.ftc.gov/os/2003/09/synovatereport.pdf>>. The two other surveys, released in July 2003, were conducted by Harris Interactive for Privacy and American Business (P&AB) and by Gartner Inc. The P&AB/Harris survey report is available at <<http://www.pandab.org>> and the Gartner survey report at <<http://www3.gartner.com/Init>>.

⁵ The FTC survey put the increase at 41%, while P&AB/Harris and Gartner both found an 80% increase from 2001 to 2002.

⁶ The FTC's report estimated the average out-of-pocket cost to victims at \$500, while the P&AB/Harris study put the average cost at \$740. The FTC estimated average time spent by victims at 30 hours. A California study by the Identity Theft Resource Center (ITRC), "Identity Theft: The Aftermath 2003," found much higher costs in time and money. The ITRC estimated that the average victim spent nearly \$1,500 on such items as telephone calls, postage, mileage, time lost from work, legal assistance, child care, translation costs, notarizing documents, and court fees. The ITRC report also found that the average victim spent 600 hours clearing up the consequences of the crime. The ITRC surveyed victims who had contacted the organization for assistance and who may have been experiencing more serious problems than those of the randomly sampled victims in the FTC's study. The ITRC report is available at <www.idtheftcenter.org>.

⁷ The Identity Theft Resource Center estimated the cost to business as much higher, in excess of \$279 billion, based on average loss per victim of more than \$92,000. The ITRC says that the difference may be explained by the fact that their interviewers were experienced identity theft assistants who spent more time with each respondent than the survey company used by the FTC.

⁸ See FTC, *Identity Theft Survey Report* (September 2003), pages 6-8.

⁹ This formulation of the security safeguards principle is from the Organisation for Economic Cooperation and Development (OECD)'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at <<http://www1.oecd.org/publications/e-book/9302011E.PDF>>.

¹⁰ FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, available at <<http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>>.

¹¹ The Gramm-Leach-Bliley Act, 15 USC 6801-6827, includes the Safeguards Rule, "Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information," 16 C.F.R. Part 314. The Health Insurance Portability and Accountability Act, PL 104-191, includes "Health Insurance Reform: Security Standards," 45 C.F.R. Parts 160, 162, and 164.

¹² California Civil Code Section 1798.21. The Information Practices Act, Civil Code Section 1798 et seq., imposes several specific responsibilities for protecting the security and confidentiality of records containing personal information.

¹³ See, for example, the CSI/FBI Computer Crime and Security Survey (2002 and 2003), available at <www.gocsi.com>.

¹⁴ Gerry Fitzpatrick of Deloitte & Touche, quoted in *The Register*, May 15, 2003. Deloitte's 2003 *Global Security Survey* is available at <www.deloitte.com/gfsi>.

¹⁵ A report on the Ponemon Benchmark Study on Corporate Compliance with California Law on Public Notification of Security Breach is attached as Appendix 6.

¹⁶ The internationally recognized information security standard is ISO/IEC 17799, a comprehensive set of controls comprising best practices in information security. For more information on the principles and practices of information security, see Appendix 5: Information Security Resources.

¹⁷ Effective May 26, 2002, the encryption standard approved for U.S Government organizations and others to protect higher-risk information is FIPS 197. For more information, see Appendix 5.

¹⁸ Standards for "clearing and sanitizing" equipment of data are in the U.S. Department of Defense's National Industrial Security Program Operating Manual, DoD 5220.22M, Chapter 8.306, available at <http://www.defenselink.mil/nii/org/sio/ia/diap/documents/ASD_HD_Disposition_memo060401.pdf>.

¹⁹ ISO/IEC 17799, cited in note 16 above, includes practices relating to responding to and reporting security incidents and malfunctions “as quickly as possible” (§ 6.3).

²⁰ See Appendix 4 for suggestions on computer security incident response from the California Highway Patrol’s Information Management Division.

²¹ 15 U.S.C. Section 7001 contains the requirements for consumer disclosure and consent to electronic notification, as required by California Civil Code Sections 1798.29(g)(2) and 1798.82(g)(2).

²² See the OECD’s *Guidelines*, cited in note 8.

²³ See Appendix 4 for definition of “computer crime” in California Penal Code Section 502(c) and suggestions on information to provide to law enforcement.

Appendix 1: Advisory Group List

Advisory Group to Office of Privacy Protection on Recommended Practices on Notice of Security Breach

Brent Barnhart
Senior Counsel
Kaiser Foundation Health Plan, Inc.

Camille Busette
Senior Policy Manager
Intuit

Dianne Carpenter
Senior Attorney
J.C. Penney Corporation
California Retailers Association

James Clark
California Bankers Association

Mari Frank
Attorney, Privacy Consultant and Author

Beth Givens
Director
Privacy Rights Clearinghouse

Roxanne Gould
Vice President, CA Public and Legislative Affairs
American Electronics Association

Chief Kevin Green
California Highway Patrol

Craig Grivette
Deputy Secretary for Business
Enterprise Technology
Business, Transportation and Housing Agency

Tony Hadley
Experian

Gail Hillebrand
Senior Attorney
Consumers Union

Clark Kelso
State Chief Information Officer

Barbara Lawler
Chief Privacy Officer
Hewlett-Packard

Fran Maier
Executive Director
TRUSTe

Dana Mitchell
Counsel to Rules Committee
California State Senate

Peter Neumann
Principal Scientist
Computer Science Lab
SRI International

Dr. Larry Ponemon
Ponemon Institute

Debra Reiger
State Information Security Officer
California Department of Finance

Tim Shea
Legal Counsel
California Franchise Tax Board

Scott Shipman
Privacy Counsel
eBay

Preston Taylor
Consultant to Assemblyman Simitian
California State Assembly

Tracey Thomas
Identity Theft Resource Center

Tom Timmons
President & CEO, Spectrum Bank
President, CA Independent Bankers

Appendix 2: Sample Notice Letters

SAMPLE LETTER 1

Data Acquired: Credit card Number or Financial Account Number

Dear _____ :

I am writing to you because a recent incident may have exposed you to identity theft.

[Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]

[Name of your organization] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. We recommend that you immediately contact *[credit card or financial account issuer]* at *[phone number]* and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask *[name of account issuer]* to give you a PIN or password. This will help control access to the account

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

Equifax	Experian	Trans Union
800-525-6285	888-397-3742	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you contact the Office of Privacy Protection. The toll-free number is 866-785-9663. Or you can visit their web site at www.privacy.ca.gov. If there is anything *[name of your organization]* can do to assist you, please call *[phone number, toll-free if possible]*.

[Closing]

SAMPLE LETTER 2
(Data Acquired: Driver's License or California ID Card Number)

Dear _____ :

I am writing to you because a recent incident may have exposed you to identity theft.

[Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]

[Name of your organization] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. Since your Driver's License *[or California Identification Card]* number was involved, we recommend that you immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license. This will cut off government access to your license record. Then call the toll-free DMV Fraud Hotline at 866-658-5758 for additional information.

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

Equifax	Experian	Trans Union
800-525-6285	888-397-3742	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you contact the Office of Privacy Protection. The toll-free number is 866-785-9663. Or you can visit their web site at www.privacy.ca.gov. If there is anything *[name of your organization]* can do to assist you, please call *[phone number, toll-free if possible]*.

[Closing]

SAMPLE LETTER 3
(Data Acquired: Social Security Number)

Dear _____ :

I am writing to you because a recent incident may have exposed you to identity theft.

[Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]

[Name of your organization] is writing to you so that you can take steps to protect yourself from the possibility of identity theft.

We recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Then call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

Equifax	Experian	Trans Union
800-525-6285	888-397-3742	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft we suggest that you contact the Office of Privacy Protection. The toll-free number is 866-785-9663. Or you can visit their web site at www.privacy.ca.gov. If there is anything *[name of your organization]* can do to assist you, please call *[phone number, toll-free if possible]*.

[Closing]

Appendix 3: California Law on Notice of Security Breach

California Civil Code

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, “personal information” means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social security number.
- (2) Driver’s license number or California Identification Card number.
- (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

(f) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, “notice” may be provided by one of the following methods:

- (1) Written notice.
- (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
- (3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified

exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

- (A) E-mail notice when the agency has an e-mail address for the subject persons.
- (B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.
- (C) Notification to major statewide media. (h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- (1) Social security number.
- (2) Driver's license number or California Identification Card number.
- (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, “notice” may be provided by one of the following methods:

- (1) Written notice.
- (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
- (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

- (A) E-mail notice when the person or business has an e-mail address for the subject persons.
- (B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
- (C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.83. Any waiver of the provisions of this title is contrary to public policy, and is void and unenforceable.

1798.84. (a) Any customer injured by a violation of this title may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

Appendix 4: Reporting Computer Crimes to Law Enforcement

Law Enforcement Contacts for Computer Crimes

California High Technology Theft and Apprehension Program

This program funds five regional task forces staffed by investigators from local, state and federal law enforcement agencies who have received specialized training in the investigation of high technology crime and identity theft investigations. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or is the target of a criminal act.

Sacramento Valley Hi-Tech Crimes Task Force
Telephone: 916-874-3002
www.sachitechcops.org

Southern California High Tech Task Force
Telephone: 562-345-4260

Northern California Computer Crimes Task Force
Telephone: 707-253-4500
www.nc3tf.org

Rapid Enforcement Allied Computer Team (REACT)
Telephone: 408-494-7186
<http://reacttf.org>

Computer and Technology Crime High-Tech Response Team (CATCH)
Telephone: 619-531-36601
<http://www.catchteam.org/>

FBI

Local Office: <http://www.fbi.gov/contact/fo/fo.htm>

National Computer Crime Squad
Telephone: 202-324-9161
E-mail: nccs@fbi.gov
<http://www.emergency.com/fbi-nccs.htm>

NIPC

National Infrastructure Protection Center
U.S. Department of Homeland Security
Online Reporting: <http://www.nipc.gov/incident/incident.htm>
Telephone: 202-323-3205
Toll-Free Telephone: 888-585-9078
E-mail: nipc.watch@fbi.gov

U.S. Secret Service

Local Office: <http://www.treas.gov/usss/index.shtml>

Reporting a Computer Crime to Law Enforcement

Guidance from the California Highway Patrol Information Management Division

When reporting a computer crime be prepared to provide the following information:

- Name and address of the reporting agency.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.)
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- Make/model of the affected computer(s).
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).
- Operating System of the affected computer(s).
- Location of the affected computer(s).

Incident Response DOs and DON'Ts

DOs

1. Immediately isolate the affected system to prevent further intrusion, release of data, damage, etc.
2. Use the telephone to communicate. Attackers may be capable of monitoring E-mail traffic.
3. Immediately notify an appropriate law enforcement agency.
4. Activate all auditing software, if not already activated.
5. Preserve all pertinent system logs, e.g., firewall, router, and intrusion detection system.
6. Make backup copies of damaged or altered files, and keep these backups in a secure location.
7. Identify where the affected system resides within the network topology.
8. Identify all systems and agencies that connect to the affected system.

9. Identify the programs and processes that operate on the affected system(s), the impact of the disruption, and the maximum allowable outage time.
10. In the event the affected system is collected as evidence, make arrangements to provide for the continuity of services, i.e., prepare redundant system and obtain data back-ups. To assist with your operational recovery of the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

DON'Ts

1. Don't delete, move, or alter files on the affected systems.
2. Don't contact the suspected perpetrator.
3. Don't conduct a forensic analysis.

California Penal Code Definition of "Computer Crime"¹

As defined by California Penal Code Section 502, subsection (c), a computer crime occurs when a person:

- (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
- (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- (3) Knowingly and without permission uses or causes to be used computer services.
- (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- (5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
- (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
- (8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

- (9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

Notes

¹ Other violations of California or federal law may also be involved in an incident of unauthorized acquisition of personal information. California laws that may be involved include identity theft (Penal Code § 530.5), theft (Penal Code § 484), or forgery (Penal Code § 470).

Appendix 5: Information Security Resources

CERT®, “Security Improvement Modules,” available at < <http://www.cert.org/security-improvement/index.html#practices> >.

Federal Trade Commission, “Financial Institutions and Customer Data: Complying with the Safeguards Rule,” available at <<http://www.ftc.gov/bcp/online/pubs/buspubs/safeguards.htm> >.

Federal Trade Commission, “Security Check: Reducing Risks to Your Computer Systems,” available at < <http://www.ftc.gov/bcp/online/pubs/buspubs/security.htm> >.

“Health Insurance Reform: Security Standards; Final Rule,” 45 CFR Parts 160, 162 and 164, available at <<http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>>.

Internet Security Alliance, “Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices,” (July 2002), available at <<http://www.isalliance.org/news/requestform.cfm> >.

National Institute for Standards and Technology (NIST) Computer Security Resource Center at <www.csrc.nist.gov>.

State Administrative Manual, Sections 4840-4845: Security and Risk Management, available at < <http://sam.dgs.ca.gov/TOC/4800/default.htm> >.

Appendix 6: Benchmark Study

2003 Benchmark Study of Corporate Compliance with the New California Law on Notification of Security Breach

Prepared by Dr. Larry Ponemon, August 28, 2003

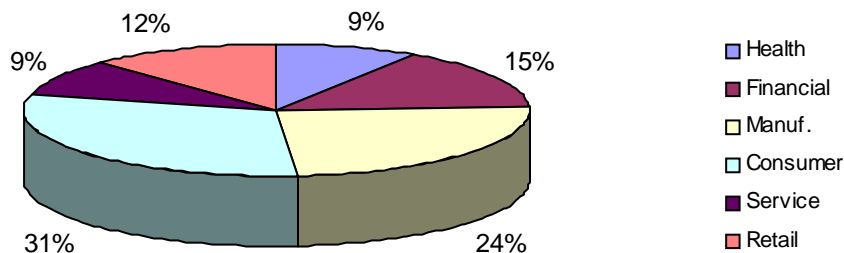
Executive Summary

Ponemon Institute is pleased to present the summary results of a preliminary benchmark study of corporate response to the new California law for notification of data security breaches (effective July 1, 2003). This current study was conducted jointly with sponsorship from Internet Security Solutions (ISS). We anticipate that results from the study will provide a meaningful baseline for measuring and monitoring trends in how leading organizations are responding to new regulatory requirements as required by California state law (civil code sections 1798.29 and 1798.82-1798.84).

The current benchmark study was conducted through confidential interviews using a fixed form design with a representative group of either privacy or information security leaders representing 34 companies. All participating individuals and companies volunteered without compensation. All companies were promised complete anonymity, and no company identification information was collected.

In total, 71 business (and governmental) organizations were contacted in July 2003 by the researcher to enroll participants in this study. The criteria for participation was twofold: (a) applicability of the new California law to the company's current operations and (b) the organizational position of the respondent with respect to domain-specific knowledge about data protection or information security practices within his or her company.

All 35 companies contacted by the researcher agreed to participate in the required timeline. One company was removed from the final analysis based on incomplete responses, resulting in a final study of 34 businesses with the following industry representation.



While most companies were large (Fortune 500 organizations), eight companies were medium sized organizations (less than \$1 billion in annual revenues).

The interviewer asked respondents a series of questions from a fixed form instrument to glean information about how organizations were responding to the new California law on notification of a security breach. Information about communication processes, organization structure, enabling

technologies and attitudes about compliance with the new law were asked. Specific drill-down questions about the information security technology to enhance compliance with the notification security breach law were pursued (not reported here).

Based on preliminary findings, many corporations are approaching their compliance with the new California law with only minor or insignificant changes being made to the communication process and technology infrastructure. As noted below, 76% of respondents said that the law motivated their companies to change the process for communicating a data security breach, yet more than 35% view these changes as relatively insignificant or immaterial to the process that was in-place before the law.

While not captured in the Tables below, several respondents mentioned that the proper handling of notice or communications at the time of crisis (such as a security breach of sensitive personal information) is an opportunity to show key stakeholders that the company will do the “right” thing with the data entrusted to them. They also acknowledged that the improper execution of notice would sorely impact the company’s brand or image in the marketplace.

A large number of respondents seem to have a compliance mindset when it comes to managing the required notice and communications process. Some feel that the process in-place today is mere form over substance because it does little to protect the customer or employee. Despite a negative view by some, the majority of companies have decided to go beyond required California residents, implementing the revised notification on an enterprise-wide (national or global) basis.

The following tables summarize the main questions and results of our study.

Table 1A shows that the largest segment of participating companies are implementing an enterprise procedure for communicating data security breaches, as opposed to a segmented approach just for California residents.

Table 1A:

The security breach communications process within your company as required by CA law pertains to:

	Freq.	Pct%
California residents	7	21%
All individuals in the U.S.	14	41%
All individuals (global)	4	12%
Not decided as yet	8	24%
No comment	1	3%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

Table 1B shows that the majority of companies consider all personal information as part of the required notification. This view goes beyond the limited variables cited in the regulation. However, 18% of respondents appear to view the new law as applying to customer or consumer information only (which could be a compliance breach).

Table 1B:

Security breach communications program pertains to:

	Freq.	Pct%
All records about individuals and households	20	59%
All records about individuals	8	24%
Only customers & consumers	4	12%
Only customers	2	6%
Only employees	0	0%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

Table 2 shows that most companies have changed or updated their process for notice of a security breach as a direct result of the new California law.

Table 2:

Did your company's communication process for data security breaches change as a result of the new law?

	Freq.	Pct%
Yes	26	76%
No	5	15%
Unsure	3	9%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

In corroboration of the above finding, Table 3 shows that 79% of respondents believe that the new law will increase the need for resources in order to achieve reasonable compliance.

Table 3:

Do the requirements of the CA law require your organization to incur additional resources?

	Freq.	Pct%
Yes	27	79%
No	4	12%
Unsure	3	9%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

Table 4 shows that more than half consider resource requirements under the new law to be moderate or insignificant. Only 15% of participants view this required increase in resources as significant.

Table 4:

How substantial are resource requirements in order to comply with the new CA law?

	Freq.	Pct%
Significant	5	15%
Moderate	8	24%
Insignificant	12	35%
Unsure	9	26%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

Items contained within Tables 5A, 5B and 5C show that many participants are still uncertain about the IT infrastructure impact of the California law.

About 32% of respondents believe that perimeter controls (such as firewalls and other devices) have changed (or will soon change) as a result of compliance requirements with the new law.

Table 5A:

Did your company's perimeter control processes change as a result of the new law?

	Freq.	Pct%
Yes	11	32%
No	8	24%
Unsure	15	44%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

Again, 32% of subjects believe that IDS or related processes have changed (or will soon change) or have been improved as a result of the new California law (Table 5B).

Table 5B:

Did your company's intrusion detection systems (IDS) change as a result of the new law?

	Freq.	Pct%
Yes	11	32%
No	10	29%
Unsure	13	38%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

More than 41% of respondents believe that the use of encryption technologies changed (or will soon change) as a direct result of new compliance requirements in California.

Table 5C:

Did your company's use of encryption change as a result of the new law?

	Freq.	Pct%
Yes	14	41%
No	15	44%
Unsure	5	15%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

As noted in Table 6A, the operating structure for managing notice requirements varies among the 34 benchmark companies. While 44% of respondents state that their companies have centralized control of breach communications, more than 21% believe that their companies have either ad hoc control or no clear procedures in place.

Table 6A:

What is the organization structure for ensuring communications for data security breaches are compliant with the new law?

	Freq.	Pct%
Centralized control process in-place	15	44%
Partially centralized control process in-place	7	21%
Decentralized control process in-place	5	15%
Informal (ad hoc) control process in-place	3	9%
No clear control process in-place	4	12%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

Table 6B shows a large variance in who is in-charge of the notice of security breaches within their organizations today. As can be seen, 24% of respondents state that "no one" is currently responsible for this important function.

Table 6B:

Who is in-charge of the data security breach communication process within your organization?

	Freq.	Pct%
No one	8	24%
IT leader	7	21%
Privacy Officer (or CPO)	6	18%
Security Office (or CISO)	5	15%
General Counsel or associate	4	12%
Chief Information Officer	1	3%
Communications or public affairs	2	6%
Other	1	3%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

Table 7A shows that 62% have a specified timeline for executing required notice and communications in the case of a security breach defined under California law.

Table 7A:

Does your company have a specific timeline for executing notice to individuals subject to communication under the new law?

	Freq.	Pct%
Yes	21	62%
No	10	29%
Unsure	3	9%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

For those who answered “yes” to the above question, Table 7B shows that for 71% of respondents the specified time limit is 10 days or less after a known breach has occurred. However, most respondents said this specified time is an internal metric subject to delay based on the investigation and enforcement process.

Table 7B:

Is your company’s the timeline for executing notice about a data security breach less than 10 business days?

	Freq.	Pct%
Yes	15	71%
No	6	29%
Unsure	0	0%
<i>Totals:</i>	<i>21</i>	<i>100%</i>

Table 8 shows that more than 47% of respondents state that the use or collection of SSN or SIN information has changed (or will soon change) as a direct consequence of the new law.

Table 8:

Did your company’s use of social security numbers (SSN and SIN) change as a result of the new law?

	Freq.	Pct%
Yes	16	47%
No	14	41%
Unsure	4	12%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

Table 9 shows that 29% of respondents believe the company’s use of encryption is sufficient to warrant safe harbor status under the new law. However, this belief varies considerably based on the technical background of the responding individual. Specifically, individuals with 10 of the 12 “yes” respondents were individuals with non-technical backgrounds (typically a lawyer or compliance officer). In contrast, 9 of the 10 “no” respondents were information security specialists with significant IT background.

Table 9:

Do your current encryption procedures over individual data warrant the safe harbor provision under the new CA law?

	Freq.	Pct%
Yes	10	29%
No	12	35%
Unsure	12	35%
<i>Totals:</i>	<i>34</i>	<i>100%</i>

The questions in Table 10A and Table 10B focus on data sharing with third parties or affiliates. In general, respondents were uncertain about how their companies manage (or plan to manage) notice about data security breaches resulting from events, errors or abuses caused by an external party such as vendors, outsourced contractors and so forth.

Table 10A shows that 41% of respondents do not plan to expand current compliance requirements for notice of a data security breach to third parties. Another 21% of respondents are uncertain about changing compliance requirements for third parties.

Table 10A:

Does your company's notice of a security breach as required under the new law pertain to exposed data shared with third parties or affiliates?

	Freq.	Pct%
Yes	13	38%
No	14	41%
Unsure	7	21%
Totals:	34	100%

Table 10B shows that 38% of respondents review (or plan to review) business partners (and other third parties) with respect to their internal compliance procedure for the provision of notice; however, such due diligence procedures appear to be either informal or superficial. Over 32% admit to doing no due diligence for data protection compliance beyond the initial contract phase.

Table 10B:

Do you review (or plan to review) business partners' compliance with the new California law?

	Freq.	Pct%
Yes	13	38%
No	11	32%
Unsure	10	29%
Totals:	34	100%

Table 11 shows that 32% of companies changed (or plan to change) their confidential communication procedures with law enforcement authorities as a result of the new law in California. However, a large number of respondents (21%) are still uncertain about how law enforcement should be brought into the investigation and enforcement process.

Table 11:

Did the new law change your company's process or procedures for communicating a data security breaches with law enforcement authorities?

	Freq.	Pct%
Yes	11	32%
No	16	47%
Unsure	7	21%
Totals:	34	100%

Table 12A summarizes the core compliance question for the benchmark sample. As can be seen, 48% of subjects are at least moderately confident that their organizations are in reasonable compliance with the notice requirement. However, 32% are either not confident about compliance or admit to being non-compliant with the law. A large percentage of participants (21%) declined to comment.

Table 12A:

As of today, how confident are you that your company is in reasonable compliance with the law CA law?

	Freq.	Pct%
Very confident	1	3%
Confident	7	21%
Moderately confident	8	24%
Not confident	10	29%
Not in compliance	1	3%
No comment	7	21%
Totals:	34	100%

Table 12B provides the frequency and percentage for six companies headquartered in California. As can be seen, of the six participants, five are either confident or very confident that their organizations are in reasonable compliance with the new law.

Table 12B:

As of today, how confident are you that your company is in reasonable compliance with the law CA law?

	Freq.	Pct%
Very confident	1	17%
Confident	4	67%
Moderately confident	0	0%
Not confident	1	17%
Not in compliance	0	0%
No comment	0	0%
<i>Totals:</i>	6	100%

Table 12C provides the frequency and percentage for companies in regulated industries that already require a data security breach communication (i.e., financial services under GLB Safeguards Rule and healthcare under HIPAA). Of the eight regulated companies, seven are at least moderately confident that their organizations are in reasonable compliance with the new law.

Table 12C:

As of today, how confident are you that your company is in reasonable compliance with the law CA law?

	Freq.	Pct%
Very confident	1	13%
Confident	5	63%
Moderately confident	1	13%
Not confident	1	13%
Not in compliance	0	0%
No comment	0	0%
<i>Totals:</i>	8	100%

Table 13 summarizes respondents' opinions about the law. It is interesting to note that 74% believe the new law in California will be repealed or significantly changed. The main reason for this belief is the apparent cost versus benefits for business and the public.

Table 13:

Do you believe that the new CA law will be repealed or significantly changes over time?

	Freq.	Pct%
Yes	25	74%
No	5	15%
Unsure	4	12%
<i>Totals:</i>	34	100%

Please do not quote or share this document without express written permission. If you would like to obtain a complimentary copy of the full report, please contact us by letter, phone or e-mail:

Ponemon Institute
 Attn: Research Department
 3901 S. Escalante Ridge Place
 Tucson, Arizona 85730
 520.290.3400
research@ponemon.org